EXHIBIT 1

22-cv-03580-WHO
United States District Court, Northern District of California

Doe v. Meta Platforms, Inc.

Decided Sep 7, 2023

22-cv-03580-WHO

09-07-2023

JOHN DOE, et al., Plaintiffs, v. META PLATFORMS, INC., et al., Defendants.

WILLIAM H. ORRICK, UNITED STATES DISTRICT JUDGE

ORDER ON MOTION TO DISMISS

WILLIAM H. ORRICK, UNITED STATES DISTRICT JUDGE

Plaintiffs challenge defendant Meta Platform, Inc.'s alleged use of proprietary computer code to obtain certain healthcare-related information of Facebook users: according to plaintiffs, the Meta Pixel allows Meta to intercept personally identifiable medical information and the content of patient communications from Facebook users, which Meta then monetizes for its own financial gain. Plaintiffs have brought several federal and state law claims, some of which they have plausibly alleged and others which need more specificity. As explained below, Meta's motion is GRANTED in part and DENIED in part.

BACKGROUND

Plaintiffs are five Facebook users who are proceeding anonymously due to the sensitive nature of this litigation. Consolidated Class Action Complaint ("CCAC," Dkt. 185) ¶¶ 24-28. They allege that Meta improperly acquires their confidential health information in violation of state and federal law and in contravention of Meta's own policies regarding use and collection of Facebook users' data. *Id.* ¶¶ 1-2, 5, 7.

Each of plaintiffs' healthcare providers-MedStar Health System, Rush University System for Health, WakeMed Health & Hospitals, Ohio State University Wexner Medical Center, and North Kansas City Hospital-allegedly installed the Meta Pixel on its patient portals. *See id.* ¶¶ 24-28. Plaintiffs claim that when they logged into their
2 patient portal on their medical provider's *2 website, the Pixel transmitted information to Meta. *Id.* ¶¶ 6, 8-13, 22. They contend that this information, contemporaneously redirected to Meta, revealed their status as patients and was monetized by Meta for use in targeted advertising. *Id.* ¶¶ 9, 13.

Plaintiffs initially moved for a preliminary injunction. Dkt. No. 46. I denied that motion, finding that while plaintiffs presented sufficient evidence of a "weighty injury," the scope of their injury and technical feasibility of plaintiffs' proposed solutions were not clear and the balance of equities and public interest factors did not support injunctive relief based on the record at that juncture. Dkt. No. 159 ("PI Order").

In February 2023, Interim Class Counsel filed their Consolidated Class Action Complaint. Dkt. No. 185. In the CCAC, plaintiffs expand the scope of their suit and bring 13 claims: (1) breach of contract; (2) breach of the duty of good faith and fair dealing; (3) violation of the Electronic Communications Privacy Act ("ECPA" or

"Wiretap Act"); (4) violation of the California Invasion of Privacy Act ("CIPA"); (5) intrusion upon seclusion; (6) California constitutional invasion of privacy; (7) negligence per se; (8) trespass to chattels; (9) violation of California's Unfair Competition Law ("UCL"); (10) violation of California's Consumer Legal Remedies Act ("CAFA"); (11) larceny; (12) violation of California's Comprehensive Computer Data Access and Fraud Act ("CDAFA"); and (13) unjust enrichment.

Defendant has moved to dismiss each of the claims asserted in the CCAC.[1]

[1] In moving for a preliminary injunction, plaintiffs relied on their claims under the ECPA, CIPA, and California tort law. Dkt. No. 46.

LEGAL STANDARD

Under FRCP 12(b)(6), a district court must dismiss a complaint if it fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion to dismiss, the plaintiff must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible when the plaintiff pleads facts that "allow the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted).
3 There must be "more than a sheer possibility that a defendant has acted unlawfully." *Id*. While courts do not *3
require "heightened fact pleading of specifics," a plaintiff must allege facts sufficient to "raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555, 570.

In deciding whether the plaintiff has stated a claim upon which relief can be granted, the Court accepts the plaintiff's allegations as true and draws all reasonable inferences in favor of the plaintiff. *See Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). However, the court is not required to accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Sec. Litig*., 536 F.3d 1049, 1055 (9th Cir. 2008). If the court dismisses the complaint, it "should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000). In making this determination, the court should consider factors such as "the presence or absence of undue delay, bad faith, dilatory motive, repeated failure to cure deficiencies by previous amendments, undue prejudice to the opposing party and futility of the proposed amendment." *Moore v. Kayport Package Express*, 885 F.2d 531, 538 (9th Cir. 1989).

DISCUSSION

I. ELECTRONIC COMMUNICATIONS PRIVACY ACT - CLAIM 3

"The Wiretap Act prohibits the unauthorized 'interception' of an 'electronic communication.'" *In re Facebook, Inc. Internet TrackingLitig*., 956 F.3d 589, 606-07 (9th Cir. 2020), cert. denied sub nom. *Facebook, Inc. v. Davis*, 141 S.Ct. 1684 (2021) (quoting 18 U.S.C. § 2511(1)(a)-(e)). To state this claim, plaintiffs must plausibly allege that Meta (1) intentionally (2) intercepted (3) the contents of (4) plaintiffs' electronic communications (5) using a device. *See In re Pharmatrak, Inc*., 329 F.3d 9, 18 (1st Cir. 2003) (listing ECPA elements).

A. Intent

Addressing the intent and intercept elements of the ECPA claim in the PI Order, I wrote:

> "Intercept" is defined under the Wiretap Act as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Although the statute does not define "acquisition," the Ninth Circuit has construed the term according to its ordinary meaning as the "act of acquiring, or coming into possession of [.]" *United States v. Smith*, 155 F.3d 1051, 1055 n.7 (9th Cir. 1998).
>
> 4 *4
>
> "Such acquisition occurs when the contents of a wire communication are captured or redirected in any way." *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (internal citation and quotation marks omitted).
>
> According to plaintiffs, the Pixel is "designed for the very purpose of intercepting communications on third-party websites by surreptitiously and contemporaneously redirecting these communications to Meta." Mot. at 11 (citing Smith Decl. ¶¶ 7-14). Plaintiffs have put forward evidence that Meta receives information through the Pixel. *See, e.g.*, Smith Decl. ¶¶ 4-5, 32-33. Meta does not dispute that the intentional or interception elements are met. See Opp. at 20-21. Plaintiffs appear likely to succeed on these two elements of their claim.

PI Order at 18.

Meta points out that it did not dispute the intent element at the preliminary injunction stage. It disputes it now, arguing that plaintiffs have failed to plausibly allege that Meta intentionally - meaning "purposefully and deliberately and not as a result of accident or mistake," *United States v. Christensen*, 828 F.3d 763, 790 (9th Cir. 2015) - intended to intercept their sensitive health information. It asserts that plaintiffs cannot meet this burden because the CCAC acknowledges that third-party web developers, not Meta, choose whether to install Pixel and also set parameters on what information to send to Meta. It also argues that intent cannot be alleged because, as plaintiffs acknowledge, Meta seeks to avoid receiving sensitive information by contractually forbidding developers from sending it and filtering out any potentially sensitive data it detects on the back end. Mot at 5-6 (citing CCAC ¶¶ 39, 44-46 (Pixel is customizable per instructions provided by Meta), 118, 125, 148-149 (Meta has systems in place to filter sensitive information and, has publicly stated it does not want sensitive health information)).

While plaintiffs acknowledge that Meta may tell third parties and Facebook users that it intends to prevent receipt of sensitive health information, plaintiffs contend that is not what Meta *really* intends. *See, e.g.*, CCAC ¶¶ 122-123, 144-146, 150, 161 (plaintiffs allege Meta's tools and filters are not effective, not fully implemented, and call into question Meta's true intent). What Meta's true intent is, what steps it actually took to prevent receipt of health information, the efficacy of its filtering tools, and the technological feasibility of implementing other measures to prevent the transfer of health information, all turn on disputed questions of fact
5 that need development on a full evidentiary record. *See, e.g., Lopez v. Apple, Inc.*, 519 F.Supp.3d 672, 684 *5 (N.D. Cal. 2021) ("At the pleading stage, however, interception may be considered intentional 'where a defendant is aware of the defect causing the interception but takes no remedial action.'") (quoting *In re Google Assistant Priv. Litig.*, 457 F.Supp.3d 797, 815 (N.D. Cal. 2020)). At this stage, intent has been adequately alleged.

B. Content

Meta also argues that plaintiffs have not and cannot plausibly plead interception of covered "content." The statute broadly defines "content" to include "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). "Contents" refers to the "intended message conveyed by the

communication"-it does not include record information regarding the characteristics of the message that is generated in the course of the communication. *See In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). For instance, contact information provided as part of a sign-up process constitutes "content" because this information is the subject of the communication. *Id*. at 1107 ("Because the users had communicated with the website by entering their personal medical information into a form provided by the website, the First Circuit correctly concluded that the defendant was disclosing the contents of a communication."). And while a URL that includes "basic identification and address information" is not "content," a URL disclosing a "search term or similar communication made by the user" "could constitute a communication" under the statute. *Id*. at 1108-09.

In the PI Order, I found that plaintiffs had made a strong showing on this element:

> In my view, the log-in buttons and the kinds of descriptive URLs identified in the Smith Decl. are "contents" within the meaning of the statute. Unlike in *Zynga*, the URLs at issue here would not merely reveal the name of a Facebook user or group-as Smith explained, the transmitted URLs include both the "path" and the "query string." Smith Decl. ¶¶ 50-51; see also *Id.* ¶ 189 (showing hardfordhospital.org/services/digestive-health/conditions-we- treat/colorectal-small-bowel-disorders/ulcerative-colitis URL).
>
> These items are content because they concern the substance of a communication. *See Zynga*, 750 F.3d at 1107; *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 137 (3d Cir. 2015) ("If an address, phone number, or URL is . . . part of the substantive information conveyed to the recipient, then by definition it is 'content.'"); *see also In re Google RTB Consumer Priv. Litig.*, No. 21-cv-2155-YGR, 2022 WL 2165489, at *10 (N.D. Cal. June 13, 2022) (finding that categories of the website, categories that describe the current section of the website, and referrer URL that caused
>
> 6 *6
>
> navigation to the current page constituted "content").

PI Order at 19. Meta acknowledges this prior conclusion, but argues that unspecified "remaining items" that are transferred "mostly" do not qualify as content and claims based on "those communications" should be dismissed. Mot. at 9-10; Reply at 4.

At this juncture, plaintiffs have adequately alleged covered content is transferred. The boundaries of what transferred information is content under the Act is better determined on a full evidentiary record.

C. Consent

Finally, Meta argues that the ECPA's one-party consent exemption (exempting liability for intercepted information resulting from one party's consent) bars the claim as a matter of law. Meta points out, again, that it is the third-party web developers who make their Pixel-enhanced websites available to plaintiffs and their other healthcare customers, and by doing so those healthcare entities have necessarily consented to the transmission of data to Meta.

In the PI Order, I explained:

[T]he Wiretap Act exempts liability in certain circumstances. The statute provides that:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d). In other words, the Wiretap Act allows interception where the interception is made by a "party" to the communication or where a "party" has consented to the interception. *Id.* This exception does not apply, however, where the interceptor acts "for the purpose of' committing any crime or tort in violation of state or federal law. *Id.*

7 PI Order at 20.[2] *7

[2] In the PI Order, I "put aside" the issue of consent and considered whether the "crime or tort" "exception to the exception" applied. I concluded there was a "not-insignificant chance, then, that plaintiffs may be able to show that the crime-tort exception applies," but "in light of the authority in this district finding that liability does not lie where a defendant's primary motivator was to make money, I am not convinced that plaintiffs have met their burden to show that the law and facts 'clearly favor' their position." *Id*. at 20-22. However, I noted "this claim will present differently in a motion to dismiss context," and recognized that the "parties will have the opportunity to refine their arguments regarding Meta's purpose in intercepting the information at issue here later in the litigation." PI Order at 20-22.

On this motion to dismiss, the issue of consent is front and center and the burden of proof to show this exemption applies is on Meta. *See In re Google RTB Consumer Priv. Litig*., 606 F.Supp.3d 935, 949 (N.D. Cal. 2022). In support of dismissal, Meta relies on *Katz-Lacabe v. Oracle Am., Inc*., No. 22-CV-04792-RS, 2023 WL 2838118, at *10 (N.D. Cal. Apr. 6, 2023). There, plaintiffs challenged Oracle's collection of "personal information from internet users" by "synchroniz[ing] that data to create individual profiles, and ultimately sell[ing] that data- bolstered by data made available by its partners-on its Data Marketplace." The court dismissed the ECPA claim because, "[a]s Defendant's customers must have chosen to deploy Oracle's tools on their websites, it necessarily follows that 'one of the parties to the communication'-the websites themselves-gave 'prior consent to such interception.'" *Id*. at *210 (relying on *Rodriguez v. Google LLC*, No. 20-cv-04688-RS, 2021 WL 2026726, at *6 (N.D. Cal. May 21, 2021).

Plaintiffs counter with *Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at *9 (N.D. Cal. Aug. 7, 2023). There, the court rejected summary judgment on the consent issue under the ECPA claim, despite the defendant having "generally disclosed" its data tracking practices, because it also "promote[d] the privacy afforded by Incognito" as a browsing mode. *Id*. In that situation, Google "itself created a situation where there is a dispute as to whether users' consent of Google's data collection generally is 'substantially the same' as their consent to the collection of their private browsing data in particular." *Id*.

The facts alleged here - that while Meta disclosed its purported attempts to prevent third-party developers who incorporated the Pixel from sending sensitive data to Meta, Meta in fact intended to receive and did receive that sensitive data - bring this case closer to *Brown*. *Id*., 2023 WL 5029899 *7 ("For consent to be actual, the disclosures must 'explicitly notify' users of the practice at issue."). Meta has not pointed to anything I can judicially notice on this motion to dismiss to show as a matter of law that the healthcare providers did not just
8 presumably but *8 *actually* consented to the sending of sensitive healthcare information of its customers. Determination of whether actual consent was given depends on what Meta disclosed to healthcare providers,

how it described and trained healthcare providers on the Pixel, and how the healthcare providers understood the Pixel worked and the information that then could or would be collected by Meta. These evidence-bound determinations are inappropriate to reach on this motion.

Meta's motion to dismiss the ECPA claim is DENIED.

II. CALIFORNIA INVASION OF PRIVACY ACT - CLAIM 4

In the PI Order, I concluded that plaintiffs had adequately alleged and supported their CIPA claim under both sections 631(a) and 632, based on Meta's challenges to "content" under 631(a) and "confidential communications" under 632. PI Order at 23-24. Meta now moves to dismiss the California state law analog to the ECPA, raising arguments not addressed in my PI Order.

A. Extraterritoriality

Meta initially argues that CIPA does not apply "extraterritorially," because CIPA's intent is "to protect the right of privacy of the people of this state." Cal. Penal Code § 630. As none of the named plaintiffs are California residents, Meta contends the CIPA claim must be dismissed.

I disagree for three reasons. First, this contention is arguably premature. *Kellman v. Spokeo, Inc.*, 599 F.Supp.3d 877, 894 (N.D. Cal. 2022), *motion to certify appeal denied*, No. 3:21-CV-08976-WHO, 2022 WL 2965399 (N.D. Cal. July 8, 2022) (deferring choice of law analyses until class certification, after discovery shed light on whether defendants' acts had a substantial nexus to California).

Second, plaintiffs have plausibly alleged that the conduct at issue, in terms of the design and marketing of the Pixel technology and development and implementation of its Terms of Service, occurred in California;. *See, e.g., Schmitt v. SN Servicing Corp.*, No. 21-CV-03355-WHO, 2021 WL 3493754, at *3 (N.D. Cal. Aug. 9, 2021) (data breach allegations regarding defendant who operated out of California "sufficient to allow out-of-state plaintiffs to seek recovery under California law"); *Valentine v. NebuAd, Inc.*, 804 F.Supp.2d 1022, 1028 (N.D. Cal. 2011) ("A legislative purpose that articulates an interest in protecting those within California *9 is not inconsistent with also allowing non-Californians to pursue claims against California residents."); *see also Oman v. Delta Air Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018), *certified question accepted sub nom. Oman v. Delta Air Lines*, No. S248726, 2018 WL 10809386 (Cal. July 11, 2018), *and certified question answered*, 9 Cal. 5th 762 (2020) ("If the conduct that 'creates liability' occurs in California, California law properly governs that conduct.").

Third, Facebook's Terms of Service specify that California law applies to disputes between Facebook and its users. CCAC ¶ 292. That alone may not be dispositive, but it supports allowing these non-resident plaintiffs to assert a claim against a California resident under CIPA. *See Maldonado v. Apple, Inc*, No. 3:16-CV-04067-WHO, 2021 WL 1947512, at *6 (N.D. Cal. May 14, 2021) ("California Supreme Court held that choice-of-law clauses in contracts are generally enforceable and laid out a multipart test to determine whether to follow the contracted-for jurisdiction's law or disregard it.").

I am not determining or foreclosing any choice-of-law issues. Choice-of-law has not been squarely raised. I am denying the motion to dismiss the CIPA claim based on Meta's exterritoriality argument.

B. Intent

Meta also argues plaintiffs fail to allege plausible facts to support the intent element of CIPA, which requires a showing of Meta's "affirmative desire" to intercept communications. Intent under CIPA is determined consistently with intent under ECPA, and for the same reasons as discussed above, intent has been adequately alleged. Whether Meta's affirmative disclosures and back-end filtering process sufficiently negate intent depends on Meta's knowledge as well as its implementation and the efficacy of its alleged contractual efforts and back-end filtering. Those will be tested on an evidentiary record. Similarly, Meta's point that Pixel captures some data that healthcare entities may permissibly share with Meta might provide a defense to some portion of plaintiffs' CIPA claim, but it does not negate the plausible allegations that sensitive healthcare information is intentionally captured and transmitted to Meta.

C. Sent or Received

10 Meta points out that CIPA only covers interception of a communication while "it is being *10 sent from, or received at any place within this state," Cal. Penal Code § 631(a), and argues plaintiffs have not plausibly alleged that plaintiffs' information was being sent to or received from a place in this state. Plaintiffs plead that Meta is headquartered in California and Meta "designed and *effectuated* its scheme to track the patient communications at issue here from California." CCAC ¶ 369 (emphasis added). That is sufficient at this stage.

D. Device

The last CIPA challenge is whether the Pixel is a "device" under Section 632(a) because it is a piece of software. Meta points out that two judges in this District, when considering "electronic tracking devices" under Penal Code section 637.7(d), have rejected the argument that tracking software are "devices." *See In re Google Location Hist. Litig.*, 428 F.Supp.3d 185, 193 (N.D. Cal. 2019) (Davila, E.) (Google maps software and related "services are not a 'device' within the meaning of Section 637.7(d)."); *In Moreno v. San Francisco Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *5 (N.D. Cal. Dec. 14, 2017) (Corley, J.) (an "electronic tracking device" does not include "software installed in mobile devices").

Plaintiffs respond that the section 637.7 cases so not apply to this section 632(a) case. They instead discuss decisions construing and interpreting CIPA consistently with the ECPA which hold that servers or software qualify as "devices" under the ECPA. Oppo. at 10 n.2.[3] Most on point is *In re Carrier IQ, Inc.*, 78 F.Supp.3d 1051, 1084 (N.D. Cal. 2015). There, plaintiffs alleged that a software application, once installed on users' phones, "surreptitiously intercepted personal data and communications and transmitted this data to Carrier IQ and its customers." *Id.* The Honorable Edward M. Chen held that "plaintiffs have sufficiently alleged that the
11 Carrier IQ Software is a 'device' for purposes of the Wiretap Act." *Id.* at 1084. The section 637.7 cases are *11 distinguishable, and absent contrary authority under section 632(a), I agree that the Pixel software is a device under section 632(a).

[3] A few of the cases plaintiffs rely on are not truly in support. For example, in *United States v. Szymuszkiewicz*, 622 F.3d 701, 707 (7th Cir. 2010), as amended (Nov. 29, 2010), the court held that the defendant "acquired the emails by using at least three devices: Infusino's computer (where the rule was set up), the Kansas City server (where the rule caused each message to be duplicated and sent his way), and his own computer (where the messages were received, read, and sometimes stored)." In *Lopez v. Apple, Inc.*, 519 F.Supp.3d 672, 690 (N.D. Cal. 2021), the court simply found that "Apple used the devices [iPhone] by programming Siri software to intercept communications when no hot word was spoken"). In both cases, devices were used. Here the use allegations concern only software.

Meta's motion to dismiss the CIPA claim is DENIED.

III. CONSTITUTIONAL PRIVACY (CLAIM 6) AND INTRUSION ON SECLUSION (CLAIM 5)

Addressing the invasion of privacy and intrusion on seclusion claim in the PI Order, I explained that plaintiffs had shown enough to demonstrate a reasonable expectation of privacy in their medical communications (despite Meta's policies generally disclosing its collection of data from users and its disclosures that it would require partners to obtain lawful rights to share protected user data) and that Meta's conduct was highly offensive. PI Order at 24-27. Meta argues here that the California's constitutional privacy protections do not apply extraterritorially and plaintiffs have failed to adequately allege their sensitive information was received by Meta.

As with CIPA, plaintiffs have plausibly alleged that the conduct causing them harm occurred in and emanated from California. That is sufficient at this juncture.

Concerning the protected interest, Meta argues that plaintiffs have failed to plausibly allege a violation of their constitutionally protected privacy interests because the named plaintiffs fail to identify with specificity what, if any, private or particularly sensitive information about them Meta allegedly received. Meta is correct that these named plaintiffs do not identify in the CCAC what specific, personal or private information they conveyed to their healthcare providers that they reasonably believe Meta received.

In opposition, plaintiffs do not dispute this or identify any particular categories of information that they shared with their healthcare providers that they reasonably believe was captured by Meta. Instead, they rely on *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020) to argue they do not need to disclose the specific information they contend Meta received. But in that case, there was no dispute that Facebook collected "a full-string detailed URL, which contains the name of a website, folder and sub-folders on the web-server, and the name of the precise file requested," when it operated. *Id.* at 605. Here, as Meta repeatedly points out
12 and plaintiffs admit, there is information collected by the Pixel software that does not *12 constitute sensitive, personal information.

Given the nature of this case - where plaintiffs allege that both unprotected and constitutionally protected information was captured by Meta's Pixel - plaintiffs are required to amend to describe the types or categories of sensitive health information that they provided through their devices to their healthcare providers. That basic amendment (which can be general enough to protect plaintiffs' specific privacy interests) will allow these privacy claims to go forward.[4]

> [4] Related to the "legally protected interest" argument, Meta also contends that the privacy claims fail because plaintiffs have not alleged a "sufficiently serious" invasion of their privacy rights. Once plaintiffs amend to identify the types of protected information they shared with their healthcare providers and was likely captured by Meta, they will have plausibly alleged a sufficiently serious impact on their privacy rights. *See* PI Order at 26-27. Meta's remaining arguments, that its filtering efforts and purported use of any received healthcare information are highly relevant to whether its conduct is "highly offensive," have merit. Mot. at 14-15. But the balancing of the various factors required by *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal.4th 1, 37 (1994), must be done on a full evidentiary record.

Plaintiffs' invasion of privacy claims are DISMISSED with leave to amend.

IV. CALIFORNIA'S COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT - CLAIM 12

CDAFA provides that only an individual who has "suffer[ed] damage or loss by reason of a violation" of the statute may bring a civil action "for compensatory damages and injunctive relief or other equitable relief." Cal. Penal Code § 502(e)(1). CDAFA permits recovery of "[c]ompensatory damages [that] include any expenditure

reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." *Id*.

A. Loss or Damage

Meta initially seeks dismissal of plaintiffs' CDAFA claim because plaintiffs have not alleged and cannot allege "damage or loss" in an action like this that is based on privacy violations as opposed to an intrusion that impacts the performance or operation of computer devices. Meta relies on a recent decision from Chief Magistrate Judge Donna M. Ryu, *Cottle v. Plaid Inc*., 536 F.Supp.3d 461 (N.D. Cal. 2021), where Judge Ryu rejected a theory of loss or damage under CDAFA based on the "loss of the right to control their own data, the
13 loss of the value of their data, *13 and the loss of the right to protection of the data," as that type of loss was not covered by the statute. *Id*. at 488 (citing *Nowak v. Xapo, Inc*., No. 5:20-cv-03643-BLF, 2020 WL 6822888, at *4-5 (N.D. Cal. Nov. 20, 2020) (dismissing CDAFA claim based on loss of value of stolen cryptocurrency in part because the nature of the loss was not cognizable under CDAFA)).

Plaintiffs respond that they adequately allege actionable "loss or damage" under CDAFA by alleging: (1) the Pixel "has precluded" them from being able to communicate with their healthcare providers through their computers or otherwise and (2) their protected information is diminished in value. Plaintiffs cite a number of cases from this District that they claim support these types of damages under CDAFA. However, each of the cases plaintiffs rely on dealt with different sections of CDAFA or allegations of impaired device performance. Oppo. at 13.[5]

> [5] *See In re Apple Inc. Device Performance Litig*., 347 F.Supp.3d 434, 454 (N.D. Cal. 2018), on reconsideration in part, 386 F.Supp.3d 1155 (N.D. Cal. 2019) (addressing (c)(4) and (c)(5) and allegations of device impairment); *Ubisoft, Inc. v. Kruk*, No. CV 20-478-DMG (ASX), 2021 WL 3472833, at *4 (C.D. Cal. July 9, 2021) ((c)(5) claim alleging DDoS attacks); In re Carrier IQ, Inc., 78 F.Supp.3d 1051, 1067 (N.D. Cal. 2015) (alleging impact on battery life and performance); *see also In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 599 (9th Cir. 2020) (finding Article III standing to allege CDAFA claim, but not addressing standing under the "loss or damage" requirement of the statute).

Plaintiffs provide no support for their argument that an "inability" to use their computer devices to communicate with their healthcare providers in the future is a cognizable form of loss or damage actionable under the CDAFA. Their diminished value of information claim is foreclosed by the reasoning in *Cottle*.

Plaintiffs indicated at the hearing that they might be able to plead a different theory of impairment of their computing devices. They may do so. The CDAFA claim is DISMISSED, with leave to amend.

B. Other CDAFA Elements

Meta also attacks the substance of the CDAFA claim. The CCAC relies on various substantive sections of CDAFA: sections 502(c)(1), (c)(2), (c)(3), (c)(6), (c)(7), and (c)(8). In opposition plaintiffs address only (1) and
14 (8).[6] In their further amended CCAC, plaintiffs shall *14 limit the CDAFA claim to these two subsections only.

> [6] These provisions hold persons liable for "(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data" and (8) "Knowingly introduces any computer contaminant into any computer, computer system, or computer network." Cal. Penal Code § 502(c).

Meta argues that plaintiffs have not alleged a claim under (1) because intent has not been sufficiently alleged. Consistent with the ECPA and CIPA discussions above, however, plaintiffs have adequately alleged intent. Meta next contends that plaintiffs cannot plausibly allege a claim under (8), as it was the healthcare entities' web developers who introduced Pixel onto their own websites, not Meta. Plaintiffs' allegations regarding how Meta induced or encouraged those entities to adopt and install the Pixel suffice at this juncture.

Meta also asserts that even if it could be vicariously liable, plaintiffs have not alleged and cannot plausibly allege that the Pixel is a prohibited "contaminant."[7] In *In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011) the court explained:

> 7 Cal. Penal Code § 502(12) "'Computer contaminant' means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network."

> Section 502(c)(1[2]) defines "computer contaminant" as "any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms. . . to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network." *See* Cal.Penal Code § 502(b) (10) (emphasis added). Thus, the very definition of a "computer contaminant" limits liability to conduct that occurs "without the intent or permission of the owner of the information." Moreover, the section on "computer contaminants" appears to be aimed at "viruses or worms," and other malware that usurps the normal operation of the computer or computer system. Although Plaintiffs[] are given leave to amend to clarify their allegations in an amended complaint, it is not clear to the Court how Section 502(c)(8) applies to the case at hand."

15 *Id.* at *13. *15

Whether plaintiffs can, on amendment, plausibly allege facts establishing recognized "loss or damage" sufficient to state a claim under CDAFA will also inform whether the Pixel is a contaminant that "usurps" the normal operation of plaintiffs' devices. *See also Flextronics Int'l, Ltd. v. Parametric Tech. Corp.*, No. 5:13-CV-00034-PSG, 2014 WL 2213910, at *5 (N.D. Cal. May 28, 2014) ("a plaintiff need only allege that the actions of the contaminant (modify/damage/destroy/record/ transmit) were undertaken by overcoming a technical barrier without the permission of the owner; the introduction of the contaminant to the system need not surmount the same hurdle.").

The motion to dismiss the CDAFA claim is GRANTED with leave to amend.

V. BREACH OF CONTRACT - CLAIMS 1 & 2

A. Limitation of Liability in Meta's Terms of Service

Meta argues initially that a "limitation of liability" clause in its TOS bars the breach of contract claims. That clause provides: "[Meta]'s liability shall be limited to the fullest extent permitted by applicable law, and under no circumstance will we be liable to you for any lost profits, revenues, information, or data, or consequential,

special, indirect, exemplary, punitive, or incidental damages arising out of or related to these Terms or the Meta Products." Meta RJN Ex. 1 at 7.[8]

[8] Meta seeks judicial notice of various documents, including its TOS, Business Tools Terms, Commercial Terms, Privacy Policy and Cookies Policy. *See* Dkt. No. 232-1. Plaintiffs do not oppose the request. The request is GRANTED.

Meta notes that at least one court in this District has applied Meta's limitation provision to defeat express and implied contract claims, rejecting the argument that the limitation provision was unconscionable. *See Bass v. Facebook, Inc.*, 394 F.Supp.3d 1024, 1037 (N.D. Cal. 2019) ("Perhaps regrettably, '[w]ith respect to claims for breach of contract, limitation of liability clauses are enforceable unless they are unconscionable, that is, the improper result of unequal bargaining power or contrary to public policy.' *Food Safety Net Servs. v. Eco Safe Sys. USA, Inc.*, 209 Cal.App.4th 1118, 1126, 147 Cal.Rptr.3d 634 (2012)."). The *Bass* court then determined
16 that the limitations provision was not unconscionable as applied to the contract and quasi-contract *16 causes of action. *Id.* at 1038; *see also Darnaa, LLC v. Google LLC*, 756 Fed.Appx. 674, 676-77 (9th Cir. 2018) (rejecting unconscionability argument, "[a]s interpreted by California courts, Section 1668 generally does not prohibit parties from limiting liability for breach of contract, including breach of the implied covenant. [citations omitted]. We see no reason to depart from this principle here.").

Plaintiffs respond that Meta's attempt to limit its liability for the breach claim runs afoul of California Civil Code section 1668. It provides: "All contracts which have for their object, directly or indirectly, to exempt anyone from responsibility for his own fraud, or willful injury to the person or property of another, or violation of law, whether willful or negligent, are against the policy of the law." Here, because defendants acted intentionally by refusing to stop the data transfer or employ a stronger filter mechanism, plaintiffs assert that section 1668 comes into play even for a breach of contract claim. On that basis, they distinguish *Bass* from this case as *Bass* concerned a negligent data breach case caused by an obscure flaw in Meta's code and Meta took immediate action to fix it.

In addition to the substantive differences between the allegations in *Bass* and this case, plaintiffs also note that other courts in this district have allowed breach of contract claims to continue against Facebook despite the limitation of liability clause. *See*, *e.g.*, *Lundy v. Facebook Inc.*, No. 18-CV-06793-JD, 2021 WL 4503071, at *2 (N.D. Cal. Sept. 30, 2021) ("For the damages element of plaintiffs' contract and quasi-contract claims, plaintiffs have adequately pleaded claims for disgorgement and nominal damages. [] These types of damages are not covered by the limitation of liability provision Facebook points to in its motion to dismiss. [] Nominal damages may be recovered for a breach of contract under California law." (internal citations omitted)); *Shared.com v. Meta Platforms, Inc.*, No. 22-CV-02366-RS, 2022 WL 4372349, at *4 (N.D. Cal. Sept. 21, 2022) (allowing breach of contract and other claims to proceed past motion to dismiss stage despite limitation of liability clause because the "discovery process would aid in determining more concretely whether each claim avers direct or indirect damages. The limitations provision will therefore not mandate dismissal of any of Plaintiff's claims,
17 though Defendant can always reassert the limitations provision in, for example, a motion *17 for summary judgment").

Here, plaintiffs have pleaded entitlement to nominal damages and restitution. CCAC ¶ 317. Given the differences between the damages sought as well as the intentional conduct alleged (distinguishing this case from *Bass*), the breach of contract claims will not be dismissed based on the limitation of liability clause. Meta may, however, move to limit the types of damages available (*e.g.*, anything beyond nominal damages) on summary judgment or at another appropriate juncture.

B. Sufficiently Definite Promises and Breach

Next Meta argues that the contractual provisions on which plaintiffs based their breach of contract claim are not "sufficiently definite." The specific contractual promises made in Meta's Privacy Policy and TOS and plaintiffs' allegations regarding breach are identified at paragraph 312 in the CCAC:

> • "We require Partners to have the right to .. share your information before giving it to us." Plaintiffs allege: "Meta does not require Partners to have the right to share health information with Meta before giving it to Meta."
>
> • "We employ dedicated teams around the world ... to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community."
>
> Plaintiffs allege: "Meta does not employ dedicated teams to prevent its unauthorized acquisition of health information. To the contrary, Meta employs dedicated teams to encourage health entities to share health information with Meta that the health entities lack rights to share."
>
> • "We . develop advanced technical systems to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community. If we learn of content or conduct like this, we will take appropriate action - for example . removing content, blocking access to certain features, disabling an account, or contacting law enforcement."
>
> Plaintiffs allege: "Meta has developed advanced technical systems to detect potential misuse of certain products and is fully capable of using those systems to detect Pixel Partners from which it is acquiring health information without authorization. However, Meta has not used those systems to stop acquiring such information and has not taken appropriate action to prevent health entities from sharing health information with Meta in the absence of the right to do so."

18 *18

> • "We work with external service providers, partners, and other relevant entities ... to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community, including to respond to user reports of potentially violating content."
>
> Plaintiffs allege: "Meta does not work with external service providers, Partners, or other relevant entities to detect potential misuse of sending health information to Meta through the Pixel without the right to do so. To the contrary, Meta works with Partners to help those Partners avoid the meaningless restrictions Meta places on ads that are targeted to health. As shown above, Meta teaches health entities how to avoid its "restrictions" on personalized health targeted ads by removing certain words that would give users the idea that the ad was specifically targeted to them, all the while continuing to target ads to specific users based on personal attributes, including health."

CCAC ¶ 312; *see also* ¶¶ 96-97 (noting Meta "requires" some information including sensitive and protected information from users for services to work), 117 (same).[9] Plaintiffs' specific references to identified provisions in Meta's TOS and Privacy Policy are sufficiently definite to "determine the scope of the duty and the limits of performance must be sufficiently defined to provide a rational basis for the assessment of damages." *Ladas v. California State Auto. Assn.*, 19 Cal.App.4th 761, 770 (1993).

[9] In addressing consent at the preliminary injunction stage, as both sides here note, I expressed that Meta's use of the term "require" was susceptible to multiple meanings. PI Order at 16.

Plaintiffs have also plausibly alleged that Meta breached the promises. Meta overreads the impact of plaintiffs' "admissions" that Meta may have "discouraged" partners from sending sensitive or protected information and Meta employed a filter to reduce the transfer of sensitive or protected information. Meta ignores plaintiffs' detailed and plausible allegations regarding how and why the transfer of sensitive or protected information is necessary for Meta's advertising services to function in the way Meta advertised those services, as well as allegations that Meta knew its filter was not effective and could have improved its filter or taken other steps to block the transfer of the sensitive or protected information. That is sufficient at this juncture.

The motion to dismiss the breach of contract and related breach of the duty of good faith and fair dealing
19 claims is DENIED.[10] *19

[10] Plaintiffs' covenant of good faith and fair dealing claim is based on allegations that Meta abused its power in interpreting "require" in a way that does not actually require anything. CCAC ¶ 323; Oppo. at 17. As construed, the claim is not merely duplicative of or exceeding the obligations imposed by the contractual provisions plaintiffs rely on for their express breach claim. Plaintiffs have also adequately Meta's intent - conscious and deliberative acts - given the breach allegations discussed above. *See Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal.App.3d 1371, 1395 (Cal.Ct.App. 1990).

VI. UNJUST ENRICHMENT - CLAIM 13

Meta moves to dismiss the unjust enrichment claim, which California law construes as a quasi-contract claim, in light of plaintiffs' express contract claim. But plaintiffs may plead this claim as an alternative at this juncture, even if the contract claim can be read to cover plaintiffs' allegation that Meta sold their data without consent and unjustly retained the proceeds. *See Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015). Meta also argues that the claim cannot stand as plaintiffs have failed to plead that they lack adequate remedies at law under *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020). But plaintiffs do allege that their remedies at law are inadequate. *See* CCAC ¶¶ 448, 489.

The motion to dismiss the unjust enrichment claim is DENIED.

VII. NEGLIGENCE PER SE - CLAIM 7

Under California law, negligence per se is not a separate cause of action, but a negligence claim analyzed under the per se doctrine. *See Dent v. Nat'l Football League*, 902 F.3d 1109, 1118 (9th Cir. 2018). Under that doctrine, the standard of care can be established by a statute, and a defendant's violation of that statue can "give rise to a presumption that it failed to exercise due care" where that violation "proximately caused an injury," the injury resulted from something the statute was designed to prevent, and the person who was injured was "one of the class of persons for whose protection the statute, ordinance, or regulation was adopted." *Id.* (internal citations omitted). However, the basic elements of a negligence claim, including duty of care and causation, must still be alleged. *See Quiroz v. Seventh Ave. Ctr.*, 140 Cal.App.4th 1256, 1285 (2006).

Meta attacks plaintiffs' attempt to plead a breach of the duty of care required to state a negligence-based claim. Plaintiffs' only identified source of duty is HIPAA, and at least one court this District and another within the Ninth Circuit have rejected HIPAA as a basis of a negligence per se claim. *See, e.g., Austin v. Atlina*, No. 20-
20 CV-6363-YGR, 2021 WL 6200679, at *3 (N.D.Cal. Dec. 22, 2021) *20 ("Because there is no private right of action under HIPAA, plaintiff's HIPAA claim is not cognizable under common law"); *Teeter v. Easterseals-Goodwill N. Rocky Mountain, Inc.*, No. CV-22-96-GF-BMM, 2023 WL 2330241, at *4 (D. Mont. Mar. 2, 2023) (dismissing negligence per se cause of action based on HIPAA); *see also Delta Sav. Bank v. United States*, 265 F.3d 1017, 1026 (9th Cir. 2001) ("[t]o bring suit under the FTCA based on negligence per se, a duty must be

identified, and this duty cannot spring from a federal law. The duty must arise from state statutory or decisional law, and must impose on the defendants a duty to refrain from committing the sort of wrong alleged here," and citing authority explaining "[t]he pertinent inquiry is whether the duties set forth in the federal law are analogous to those imposed under local tort law") (quotations omitted); *In re: Netgain Tech., LLC*, No. 21-CV-1210 (SRN/LIB), 2022 WL 1810606, at *16 (D. Minn. June 2, 2022) ("Here, Plaintiffs have not cited any precedent in California, Minnesota, Nevada, South Carolina, or Wisconsin that permits a state-law negligence per se claim to proceed based on the theory that there is a violation of Section 5 of the FTC Act."); *but see In re Ambry Genetics Data Breach Litig.*, 567 F.Supp.3d 1130, 1143 (C.D. Cal. 2021) (allowing negligence/negligence per se claim based on violations of FTCA and HIPAA to proceed).[11]

[11] Meta also challenges plaintiffs' ability to plausibly please causation for a negligence claim, given plaintiffs' admission that the healthcare providers' web developers, not Meta, choose what information the Pixel sends to Meta. Mot. at 21. Given plaintiffs' plausible allegations that Meta induced or encourages web developers to send protected or sensitive private information, causation is sufficiently alleged at this juncture.

Following the majority of the cases that have considered the issue, the negligence per se claim based on a duty created by HIPAA is DISMISSED with leave to amend so that plaintiffs may attempt to identify a state law source of the duty of care.

VIII. TRESPASS TO CHATTELS - CLAIM 8

Under California law, trespass to chattels "lies where an intentional interference with the possession of personal property has proximately caused injury." *Intel Corp. v. Hamidi*, 30 Cal.4th 1342, 1350-51, 1 Cal.Rptr.3d 32, 71 P.3d 296 (2003). This claim does not lie where injuries are to privacy and confidentiality. *See Casillas v. Berkshire Hathaway Homestate Ins. Co.*, 79 Cal.App. 5th 755, 765 (2022). *21 In cases of interference with possession of personal property not amounting to conversion "'the owner has a cause of action for trespass or case, *and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use*.'" *Hamidi*, at 1351 (emphasis in original, quoting *Zaslow v. Kroenert*, 29 Cal. 2d 541, 551 (1946)); *see also id*. 1353 (where there was "no actual or threatened damage to [plaintiff's] computer hardware or software and no interference with its ordinary and intended operation," the defendant's trespass was not actionable); *In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *13-14 (N.D. Cal. Sept. 20, 2011 (following *Hamidi* and dismissing a privacy-based action where plaintiffs failed to connect the trespass to a harm in the functioning of the phone).

21

Plaintiffs' trespass claim is based on their assertions that Meta places the fbp cookie on their devices via their health-care providers' websites. They do not allege that the presence of that cookie "impairs" the operation of their devices in terms of diminished storage, decreased battery life, or otherwise. Instead, they assert that Meta's tracking diminishes the value of plaintiffs' computing devices because plaintiffs no longer want to use their devices to communicate with their healthcare providers. CCAC ¶¶ 415-28, 423-25. They analogize their inability to use their phones and computers to communicate with their healthcare providers (lest they disclose personal healthcare information) to the situation in *Grace v. Apple Inc.*, No. 17-CV-00551, 2017 WL 3232464, at *11 (N.D. Cal. July 28, 2017). There, based on allegations that Apple heavily advertised the presence and ability to use Facetime in its iPhones and allegations that use of Facetime was integral to the plaintiffs' use of their iPhones, the court allowed the trespass claim to continue because the removal of Facetime from plaintiffs' phones due to Apple's software update significantly impaired the value of plaintiffs' phones.

Here, unlike in *Grace*, there are no allegations that any functionality inherent in their computing devices has been impacted by Meta's conduct. Nor are there allegations that plaintiffs purchased any specific computing device with the purpose in whole or part of using that device to communicate with their healthcare providers. That these plaintiffs may have valued using their personal devices to communicate with their healthcare
22 providers does not sufficiently impair the *22 value of those devices to allow the plaintiffs to state a trespass to chattels claim.

The trespass claim is DISMISSED with leave to amend.

IX. LARCENY - CLAIM 11

Plaintiffs' larceny claim is brought under California Penal Code sections 484 and 496(a),[12] based on the theory that Meta "knowingly obtained" plaintiffs' information "by false pretenses." CCAC ¶¶ 455-464; Oppo. at 20-21; *see also Bell v. Feibush*, 212 Cal.App.4th 1041, 1047-48 (2013) (discussing theft by false pretenses). To plausibly state a theft by false pretenses claim, plaintiffs must allege not only that Meta made specific false representations to them, but also that plaintiffs transferred their property to Meta "in reliance on the representation." *See People v. Miller*, 81 Cal.App.4th 1427, 1440 (2000), as modified on denial of reh'g (July 6, 2000). Plaintiffs have not clearly identified the specific representations that Meta made to them that support their larceny claim or the facts showing that their reliance on those representations issufficient to state this claim.

12 California Penal Code section 484 forbids theft, which includes obtaining property "by ... false ... representation or pretense." Cal. Penal Code § 484. California Penal Code section 496(a) prohibits the obtaining of property "in any manner constituting theft." Cal. Penal Code § 496(a).

The larceny claim is DISMISSED with leave to amend.

X. UNFAIR COMPETITION LAW (CLAIM 9) AND CONSUMERS LEGAL RREMEDIES ACT (CLAIM 10)

A UCL claim may only be brought by "a person who has suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiffs, therefore, must "demonstrate some form of economic injury," such as surrendering more or acquiring less in a transaction, having a present or future property interest diminished, being deprived of money or property, or entering into a transaction costing money or property that would otherwise have been unnecessary. *Kwikset Corp. v. Superior Court*, 51 Cal.4th 310, 323 (2011).

Courts in this district have dismissed cases where, like here, the injury is based on "the loss of the inherent value of their personal data," *see Cottle v. Plaid Inc.*, 536 F.Supp.3d 461, 484 (N.D. Cal. 2021), as well as
23 where it was undisputed that plaintiffs paid no money to the *23 defendant. *See In re Facebook, Inc., Consumer Privacy*, 402 F.Supp.3d at 804 (noting "the plaintiffs here do not allege that they paid any premiums (or any money at all) to Facebook to potentially give rise to standing under California law" for purposes of UCL claim and dismissing claim for failure to allege "lost money or property"); *Wesch v. Yodlee, Inc.*, No. 20-cv-05991-SK, 2021 WL 1399291, at *6 (N.D. Cal. Feb. 16, 2021) (holding that the plaintiffs had not alleged that they "surrender[ed] more or acquir[ed] less in a transaction than they otherwise would have" for purposes of UCL standing where they had not paid money to the defendant).

Plaintiffs rely on *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F.Supp.3d 1284, 1301 (S.D. Cal. 2020). But the injury in that case was based on a "benefit-of-the-bargain" theory that plaintiffs "acquired less" in their transactions with the defendant (who sold medical devices to plaintiffs). *See also Cappello v. Walmart Inc.*, 394 F.Supp.3d 1015, 1019 (N.D. Cal. 2019) (benefit-of-the-bargain theory asserted by customers of defendant). There is no benefit of the bargain basis alleged in the CCAC with respect to the UCL claim, although benefit of the bargain allegations are made in support of the contract claim. *See* CCAC ¶ 316 (seeking benefit of the bargain contract damages). Given the different requirements to state a plausible remedy under a breach of contract claim and "loss of money or property" under the UCL, a cognizable "benefit of the bargain" theory has not adequately been alleged as a remedy for the UCL claim.[13]

[13] Plaintiffs also rely on *Callahan v. People Connect, Inc.*, No. 20-CV-09203-EMC, 2021 WL 5050079, at *19 (N.D. Cal. Nov. 1, 2021), motion to certify appeal denied, No. 20-CV-09203-EMC, 2022 WL 2132912 (N.D. Cal. June 14, 2022), but that case dealt with the misuse of names and likenesses as intellectual property.

With respect to diminished value of their data, in the most recent Northern District case to address the issue the Hon. Richard S. Seeborg reviewed recent cases and held:

> Plaintiffs fail to show they have an economic injury. Plaintiffs do identify some support for the idea that personal information without consent constitutes economic injury. *See Calhoun v. Google LLC*, 526 F.Supp.3d 605, 636 (N.D. Cal. 2021) ("[T]he Ninth Circuit and a number of district courts, including this Court, have concluded that plaintiffs who suffered a loss of their personal information suffered economic injury and had standing.") (citing cases, including *In re Facebook Privacy Litig.* ("*Facebook Privacy*"), 572 Fed.Appx. 494, 494 (9th Cir. 2014); and *In re Yahoo! Inc. Cust. Data Sec. Breach*

24 *24

> *Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017)). The weight of the authority in the district and the state, however, point in the opposite direction: that "the 'mere misappropriation of personal information' does not establish compensable damages." *Pruchnicki v. Envision Healthcare Corp.*, 845 Fed.Appx. 613, 615 (9th Cir. 2021) [citations omitted]. Because Plaintiffs have not alleged a specific monetary or economic loss, Plaintiffs lack standing to maintain their UCL claims.

Katz-Lacabe v. Oracle Am., Inc., No. 22-CV-04792-RS, 2023 WL 2838118, at *8 (N.D. Cal. Apr. 6, 2023).

Judge Seeborg relied in part on *Moore v. Centrelake Med. Grp., Inc.*, 83 Cal.App. 5th 515, 538 (2022), *review denied* (Dec. 14, 2022). There, the California Court of Appeal held that plaintiffs' "lost-value-of-PII theory, as pled, is insufficient to support UCL standing," because "[a]ppellants properly pled only that their PII was stolen and disseminated, and that a market for it existed. They did not allege they ever attempted or intended to participate in this market, or otherwise to derive economic value from their PII. Nor did they allege that any prospective purchaser of their PII might learn that their PII had been stolen in this data breach and, as a result, refuse to enter into a transaction with them, or insist on less favorable terms. In the absence of any such allegation, appellants failed to adequately plead that they lost money or property in the form of the value of their PII." *Id.* at 538.

Plaintiffs rely on *Brown v. Google LLC*, No. 20-CV-03664-LHK, 2021 WL 6064009 (N.D. Cal. Dec. 22, 2021). There, the Honorable Lucy H. Koh found that plaintiffs adequately alleged lost money or property sufficient to state their UCL claim where they alleged that "because Google previously has paid individuals for browsing histories, it is plausible that, had Plaintiffs been aware of Google's data collection, they would have demanded

payment for their data. Thus, by inducing Plaintiffs to give Google their data without payment, Google caused Plaintiffs to 'acquire in a transaction less[ ] than [they] otherwise would have.' [] Second, because there are several browsers and platforms willing to pay individuals for data, it is plausible that Plaintiffs will decide to sell their data at some point. Indeed, each named Plaintiff has alleged that he or she is aware of these browsers and platforms. [] Accordingly, by obtaining Plaintiffs' data and selling it to advertisers, Google 'diminished' Plaintiffs' 'future property interest.' *Kwikset*, 51 Cal.4th at 324.")." *Brown*, at *15. *25

Here, plaintiffs contend their allegations bring them closer to *Brown* and satisfy the deficiencies identified in *Moore*. *See* CCAC ¶¶ 22 (alleging Meta "takes patients' property and property rights without compensation and ignores their right to control the dissemination of their health information to third parties"), 215 ("Meta itself has paid users for their digital information"). But the crux of *this* case concerns Meta's receipt of "individually identifiable health information," that plaintiffs apparently do not want Meta or anyone other than their healthcare providers to have. *Id*., ¶¶ 1, 216 ("Americans typically do not want to see their individually identifiable health information for any purpose"). That brings it closer to *Moore* and *Katz-Lacabe*.

In light of the failure to separately allege a benefit of the bargain basis for "loss of money or property" under the UCL and in light of the inconsistent allegations regarding how plaintiffs could *and* would participate in a legitimate market for health care information, the UCL claim is DISMISSED with leave to amend.

There is a different deficiency with plaintiffs' claim under the CLRA. The CLRA claim is based on Meta's representation "that it required its Partners to have the right to collect, use and share Plaintiffs' and Class members' information but doing nothing to ensure their rights were protected." CCAC ¶¶ 451-453. As a result, plaintiffs allege that Meta violated section 1770(2) of the CLRA by "[m]isrepresenting the source, sponsorship, approval, or certification of goods or services"; section 1770(5) of the CLRA by "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have"; and section 1770(14) of the CLRA by "[r]epresenting that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law."

Meta moves to dismiss these misrepresentations claims under Rule 9(b) because none of the plaintiffs allege that they saw and relied on those alleged misrepresentations. *See, e.g., In re Zoom Video Commc'ns Inc. Priv. Litig*., 525 F.Supp.3d 1017, 1046 (N.D. Cal. 2021) (dismissing CLRA claims where "[n]o Plaintiff alleges reading those allegedly misleading statements, let alone reading them at a specific time or place."). Plaintiffs did not address this issue in their opposition or during the hearing. In accordance with my tentative ruling, the CLRA claim is *26 DISMISSED with leave to amend so that plaintiffs can plead facts regarding reliance on the alleged misrepresentations.[14]

[14] In my Tentative Order issued in advance of the hearing, I indicated I was inclined to follow Judge Koh's decision in *Calhoun v. Google LLC*, 526 F.Supp.3d 605, 635 (N.D. Cal. 2021). Dkt. No. 298. However, the defendant in *Calhoun* moved to dismiss arguing only that there was no property interest in browsing data and that copying data did not amount theft. *Id*. Meta's argument here rests on plaintiffs' failure to satisfy the false statement and reliance elements of that claim.

CONCLUSION

For the foregoing reasons Meta's motion is DENIED regarding the ECPA, CIPA, breach of contract, and unjust enrichment claims. The motion is GRANTED with leave to amend on the privacy, CDAFA, negligence per se, trespass, larceny, UCL, and CLRA claims. Plaintiffs shall file their amended complaint within twenty (20) days of the date of this Order.